INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# WIRELESS SENSOR NETWORK

**MISS. ANKITA K. RAMEKAR, MISS. MUKTA D. VIDHALE**

**Accepted Date: 15/03/2016; Published Date: 01/05/2016**

**Abstract:** For sensing and performing task wireless sensor network (WAS) is one of the technology. Security is an important subject nowadays in almost every network. Traditional WSNs are precious by various types of attacks like Attacks on security and authentication, Silent attacks on service integrity. Attacks on network availability. A wireless sensor netwok has important applications such as isolated environmental monitoring and target tracking. Some security issues and attacks need to be work upon. In this paper we discuss some of the issues and the denial of service attacks of security, security problems of WAS constructed on resource organized scheme and placement characteristics for designing a safe WAS.

**Keywords:** Wireless sensor Networks, Types of WSN, Sefty, Attacks

**Corresponding Author: MISS. ANKITA K. RAMEKAR**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

Ankita K. Ramekar, IJPRET, 2016; Volume 4 (9): 186-194

***PAPER-QR CODE***

## INTRODUCTION

Wireless network contains hundred and thousands of tiny sensor nodes that are low cost,low power and self-organise and perform their function in network sensor nodes and spread inside the system. WSNs can be recycled to make casual system design and action to observer the environment without want linking with wired networks. The wireless sensor network environment of communication is insecure and risky because of narrow resources and untrusted broadcast transmission media, most of security methods are not adequate in WSN but security in Wireless Sensor Network is of great significance to ensure its application success. A security scheme in WSNs must provide effective key distribution while conserving the capacity for communication among all related nodes. Considering key distribution, protected routing protocols must be considered.

**SECURITY REQUIRMENT:-** In making a strategy for WSN some security facilities such as confidentiality, authenticity, integrity, availability, newness, forward privacy and backward privacy need to be supplied.

a) **Confidentiality:** To keep the secrecy of important documents transferred between sensor node confidentiality is an essential safety service. Sensor nodes communicate complex data, so it is required to guarantee that any intruder or other adjacent network could not get personal data interrupting the transmissions. One regular safety way of providing documents confidentiality is to encrypt documents and usage of shared key so that only planned receivers can get the complex data.

b) **Authenticity**: Only providing documents confidentiality is not sufficient to guarantee the data security in WSN. As an challenger can change messages on communication or insert malevolent message, validation of data as well as sender are also vital security requirements. In the lack of authentication, attackers without difficulty are able to spread incorrect data into the wireless sensor networks.

c) **Integrity**: Integrity should be ready to guarantee that attackers cannot alter the transmitted messages. Attackers are able to create interfering packets to adjust their polarities. In adding before forwarding them a malevolent routing node can change important records in packets.

d) **Availability:** Another important ability of a WSN giving services at any time they are required is availability, besides attackers are capable to start attacks which condense the presentation of network of defeat the whole network.

**SECURITY ATTACKS:-**

WSNs are susceptible to many kinds of attacks. Rendering to the safety supplies in WSNs, these attacks can be categorized:

• Attacks on privacy and authentication: a cryptographic methods can guard the privacy and validity of communication channel from stranger assaults such as eavesdropping, packet replay attacks, and alteration or spoofing of packets.

• Attacks on availability: attacks on accessibility are often referred to as denial-of-service (DoS) attacks. DoS attacks may goal any layer of a sensor network.

For sefty of the WAS, it is essential to address the attacks and then take counter events at the plan time of WSN.

**A. Physical Attack**

This attack is also recognized as node capture. In this kind of attack, attacker's improvement full controller over some sensor nodes over straight physical access. As the price of sensor nodes must be saved as inexpensive as likely for WSN, sensor nodes with tamper proofing features are impractical. This is why sensor nodes are prone to be actually being accessed. Physical attacks have important effects on routing and entrée control tools of WSN. Example, receiving key info kept on sensor node's memory gives attacker the chance of clear admission to WSN.

For performing physical attack an opponent may require skilful knowledge, costly equipment's and other assets. Also, most of the time physical attack needs the quarry node to be impassive from the placement area for a certain quantity of time.

**B. Attacks at Different Layer**

These attacks take place affecting different networking layers of WSN.

1) **Physical Layer**

Physical layer is liable for actual documents spread and reception, frequency selection, carrier frequency generation, signalling function and documents encryption.

*1.1) Jamming*

In physical layer, jamming is a public attack that can be simply prepared by adversaries by only knowing the wireless transmission rate used in the WSN. Says the attacker transfers radio signal

casually with the equal rate as the sensor nodes are transfer signals to communicate. This radio signal affected by anothor signal directed by a sensor node and the receivers within the collection of the attacker cannot collect any message.

*2.* **Link Layer**

The data link layer is liable for the multiplexing of data stream, data frame detection, medium access, error control. This layer is susceptible to files collision when more than one sender tries to send files on only transmission channel.

*2.1. DoS Attack by Collision Generation*

In link lyear, collision is created to consume the sensor node's energy. In order to create collision, the attacker listens to the communications in WSN. When he finds out the initial of a message, he sends his own radio signal for a slight amount of time to delay with the message which roots CRC error at the receiving end, Because of this attack, the receiver cannot receive the message.

*3)* **Network Layer**

Network layer is liable for routing messages from one to another node which are neighbours or may be multi hops away for example, node to base station or node to cluster leader. network layer for WSN is frequently measured considering the rule adeptness and facts centric faces of WSN. There are numerous attacks abusing routing tools in WSN. Some aware attacks are listed here.

*3.1 Selective Forwarding*

Selective forwarding is attack where cooperated or spiteful node just falls packets of its awareness and selectively ahead packets to lessen the doubt to the neighbour nodes. The control becomes poorer when these hateful nodes are at closer to the base station . Then many sensor nodes way messages through these hateful nodes. As a importance of this attack, a WSN may give incorrect remark about the setting which affects seriously the resolution of mission serious requests such as, soldierly scrutiny and forestry fire monitoring.

*3.2) Sinkhole attack*

In sinkhole attack, a conceded node attracts a huge number of traffic of surrounding neighbours by spoofing or rerunning an poster of high class route to the base station . The attacker can do any mean action with the packets fleeting through the negotiated node.

*3.3) Wormhole Attack*

Wormhole is a dangerous attack, where the attacker receives packets at one point in the network, channels them through a fewer dormancy link than the network links to another point in the network and repeat packets there locally. This proves the national nodes of these two end points that these two unfriendly points at either end of the tunnel are very near to each other. If one end point of the channel is at close to the base station, the wormhole channel can invite important quantity of records traffic to disturb the routing and working functionality of WSN. In this case, the attack is similar to sinkhole as the adversary on the other side of the channel advertises a well route to the base station.

*3.4) Sybil Attack*

In Sybil attack, a mean or overthrew node ovens the characteristics of extra one node or constructs identity. This attack has important effect in physical routing protocols. In the place based routing protocols, nodes want to conversation place info with their neighbours to route the physically addressed packets efficiently. Sybil attack disturbs this protocol functionality concurrently being at more than one place. Self verification is the key condition for contradicting against Sybil attack. Unlike traditional networks, confirmation of individuality in WSN cannot be complete with a only shared symmetric key and public key algorithm because of computational restraint of WSN.

*4)* **Transport Layer**

In network layer end to end networks are managed.

*4.1) Flooding Attack :-*At this layer, opponents adventure the protocols that keep state at either end of the connection. For example, rival sends many joining creation needs to the victim node to finish its resources producing the Flooding attack. One answer beside this attack is to boundary the amount of networks that a node can make. But, this can stop genuine nodes to attach to the target node.

**Architecture:-**

The secure unimportant architecture consists of the succeeding phases:

1. Network topology organisation

   a. Formation

b. Inserting additional nodes into the network

c. Identifying and isolating aberrant nodes

2. Key management

3. Secure routing

3.1 Network topology organisation

3.1.1 Formation:-

The architecture of the wireless sensor network planned in this paper considers that the network is collected of sensor nodes, cluster leaders and a base station. The base station is the one border concerning the sensor network and the outside. Similar to Undercoffer et al, it is expected to function under flawless circumstances and also have adequate power and capitals to connect firmly with all nodes and outside the network. Before deployment, all sensor nodes have a unique ID and this is kept in a table situated in the base station. After deployment, the sensor nodes establish themselves into clusters by distribution their one and only one IDs and snooping for IDs being broadcast by neighbouring nodes. Upon getting a broadcast ID, each node adds this ID to its routing table Nodes that share IDs with each other then form a cluster. Each cluster then picks one sensor node to turn as cluster leader and all communication among diverse clusters must be routed through the individual cluster leader. Similarly, all communications amid nodes and the base station must also pass through the nodes' cluster leader.

3.1.2 Inserting additional nodes into the network:-

Additional nodes may be introduced into the network at any time. Before a node is inserted, the base station records and stores its unique ID and will inset the node into a cluster having the smallest number of nodes. This will help reduce the event of a cluster monopolising bandwidth if it contains a better number of nodes than other clusters who are communicating. The node will then self-organize itself within its cluster.

3.1.3 Identifying and isolating aberrant nodes

Sensor nodes that do not role as stated must be recognized and remote in order to continue the desired operation of the sensor network. An abnormal node may be the result of an attack or may act unkindly due to unexpected network behaviour. According to Hu et al. an aberrant

node is one that is not working as stated and may cease to function as predictable for the following reasons:

- It has pooped its influence source.
- It is injured by an attacker.
- It is dependent upon an intermediate node and is being deliberately congested because the intermediate node has been compromised.
- An intermediate node has been cooperated and is humiliating the communication by adapting data before advancing it.
- A node has been cooperated and communicates untrue information to the base station.

Therefore, the safety of the sensor network can be preserved by classifying an abnormal node rapidly and dividing it from the sensor network. The architecture proposed in this paper includes a protocol that is used to classify and separate abnormal nodes. This is divided into two sections:

a. node to node

b. cluster leader to node In order to define the functionality of the protocol, it will be expected that node 1 wishes to connect with node 2 whom are both situated within the similar cluster. The protocol also accepts that a secure, end-to-end communications network between node 1 and node 2 has been established. It is also expected that an attacker is not skilled of retrieving the insides of packets usual by the attacked node.

a. node to node

Node 1 will send data to node 2. Before node 1 sends a packet, it generates a nonce, adds it to the packet and protects a copy of it in memory. A different nonce is produced for each packet. Due to memory restraints in sensor nodes and the possible large number of nonce values that may essential to be generated, the nonce value will be a mixture of a random, medium-size prime number and a time stamp. Node

1 also sends a copy of the nonce value related with the packet to the cluster leader. When node 2 receives a packet, it will be obligatory to send an credit (ACK) back to node 1 within a specified time period. This ACK must comprise the same nonce that it received. Node 2 also sends a copy of this nonce value to the cluster leader.

Since the protocol adopts that an attacker cannot access the fillings of received packets, the attacker cannot admittance the nonce and therefore attach it to the ACK. covering the correct nonce back to the original sender of the packet.

When node 1 receives the ACK from node 2, it will link the nonce it receives with that it has saved in memory. If they are the same, this confirms that node 2 is not an abnormal node. Otherwise, if they are dissimilar or if no ACK has been conventional within the stated time period, it will assume node 2 is abnormal and node 1 then sends an attentive to the cluster leader. Node 1 dismisses all communication with node 2 and deletes the nonce value kept in memory. Likewise, if node 1 accepts an alert from the cluster leader representative that node2 is an abnormal node before receiving the ACK, it will directly terminate communication with node 2 and delete all nonce values saved with respect to node 2.

b. cluster leader to node

When node 1 sends packets to node 2, node 1 will send the cluster leader a copy of each nonce value for each packet. When node 2 sends an ACK back to node 1 containing the nonce value, it also sends a copy of the nonce to the cluster leader. The cluster leader will associate the two nonce values. If they are the same, it will confirm that node 2 has not been cooperated and erases the nonce values saved in memory it received from node 1 and node 2 that parallel toward the packet.

If the two nonce values are different, the cluster leader issues an aware to all nodes in the cluster that node B is an abnormal node and should be ignored. This alert is also delivered to cluster bests in all other bunches who in turn inform the nodes in their respective cluster. The base station is also warned and can take events to separate or remove node 2 from the sensor network. Similarly, if the cluster leader obtains an alert from node 1 about node 2, it transmits out the same procedures.

In a situation when the cluster leader is the sender or receiver of data with another node, then it cannot act as the self-governing party to receive nonce values and compare them to check for differences. This means that its role of cluster leader must pass to additional node that is not now involved in straight communication. This safeguards that the part of cluster lead does alteration periodically and is public between all nodes in the cluster.

**CONCLUSION**

The request for safety in WSNs converts more clear throughout skill growing of WSNs and they are used much more, however, in WSNs the node nature roots limits like limited energy,

capability of dispensation, and storage capacity. These limits create WSNs so characteristic from conservative ad hoc wireless networks. Specific approaches and protocols have been progressive to utilize in WSNs. All of the stated security hazards counting the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, offer one usual area which is for cooperating the honesty of the network they attack. The request for security in WSNs becomes more obvious during skill growth of WSNs and they are used more however, in WSNs the node environment causes limits like limited energy, capability of dispensation, and storage capacity. These limits create WSNs so characteristic from conservative ad hoc wireless networks. Specific methods and protocols have been progressive to utilize in WSNs. All of the stated safety hazards counting the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, offer one normal goal which is for cooperating the honesty of the network they attack.

**REFERENCES:**

1. Y. Wang, G. Attebury, et al. "A survey of security issues in wireless sensor networks." Computer Science and Engineering. Vol.8, no.2. 2006.
2. E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol.11, no. 6, pp. 38–43, Dec. 2004.
3. N. Gura, A. Patel, et al. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs." Cryptographic Hardware and Embedded Systems-CHES 2004, pp 925-943, 2004.
4. Razzaque, M., et al. Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. Wireless Networks and Security, Springer: 107-132, 2013.
5. A. Perrig et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks, vol. 8, no. 5, pp. 521–34, Sept. 2002.
6. H. Du, X. Hu, et al. "Energy efficient routing and scheduling for real-time data aggregation in WSNs." Computer communications. Vol.29, no. 17. 3527-3535, 2006.